PCs AND SERVERS
LIVING ON BORROWED TIME

THE END OF LIFE OF AN OPERATING SYSTEM MAY JEOPARDIZE SEVERAL BUSINESS ACTIVITIES IN A CORPORATION.

From July 14th onwards, there will no longer be either support or security patches for Windows 2003 server: your physical and virtual installations will therefore be vulnerable. However, this does not mean that you have to be subjected to a spate of incidents.

THE CHALLENGE

When support for an operating system ceases, a company's entire infrastructure is at risk, as vulnerabilities are no longer being tracked. Business continuity, confidentiality of sensitive information, corporate image and compliance with this image are all directly exposed.

These issues are magnified all the more on environments that are difficult to migrate, such as point-of-sale terminals or industrial infrastructures. This calls for a security plan designed to keep Windows Server 2003 plus the applications in working order (end of life set for July 14 th).

POSSIBLE SOLUTIONS

- Stormshield Endpoint Security, the only agent you need to install on your server or workstation
- Extended support for end-of-life OS, provided at a fee on the Microsoft platform
- System migrations, though difficult to perform within a short timeframe, and costly in terms of investment and maintenance

VARYING IMPACT DEPENDING ON ENVIRONMENT

As the months go by, due to the lack of system upgrades there will be an increase in the number of uncorrected vulnerabilities that can be exploited by hackers. The risk of production services becoming unavailable or of data being exfiltrated after an attack will increase drastically.

Infrastructures running under Windows Server 2003 R2 may potentially no longer be able to secure the exchanges required for collaborative work, file sharing, or the transfer of electronic messages. Leakage of sensitive data may also engage the legal liability of decision makers.

Similarly business activity performance on application servers will also be under threat. For example, customer relationship management, order processing, invoicing and contract management may be disrupted. At the end of the day, it is the corporate image, its responsiveness and sustainability that will be severely impacted.

OPINION

TOPIC:
SERVER PROTECTION

THE PREFERRED SOLUTION

Large organizations in Europe and North America in the defense, insurance, media, distribution and industry sectors, as well as public administrations have adopted Stormshield Endpoint Security.

Some of these clients deployed the solution in order to maintain an efficient level of security once Windows XP was no longer supported.

Gartner ranks the French vendor as a Visionary in the EPP (EndPoint Protection) market segment (December 2014).

Web: www.stormshield.eu

HIGHLIGHTS

- Detects the exploitation of vulnerabilities, including those on environments that are no longer supported
- Proactively blocks exploitation codes (Dynamic Patching)
- Proven protection against targeted attacks and APTs

Edouard Viot

Product Marketing Manager
Stormshield

> *Servers with operating systems that are no longer supported or which have not been upgraded for several years will expose datacenters and their ecosystems to unresolved security vulnerabilities. An effective countermeasure must provide permanent protection and facilitate the maintenance of compliance.*

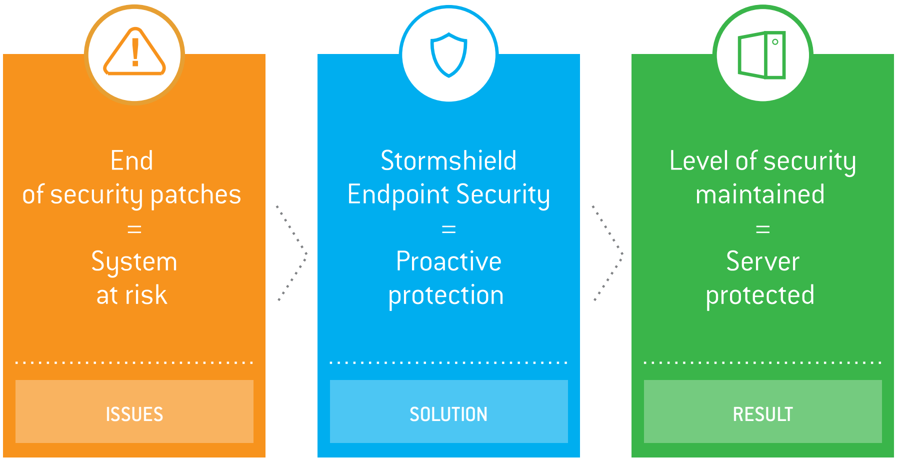
Third-party applications should also be used with caution. If a server's operating system becomes obsolete, these applications may no longer be supported either. The presence of an operating system that is no longer supported may also have a direct impact on the compliance of the information system, causing certifications such as PCI-DSS to be withdrawn or exposing the corporation to legal liability.

ADOPTING PROACTIVE SECURITY

Complementing the antivirus, Stormshield Endpoint Security's protection ensures effective and continuous protection of IT resources by preventing the exploitation of known and unknown (zero-day) vulnerabilities on operating systems and third-party applications. Based on a signatureless system, the solution provides a proactive response so as to ensure that formerly supported environments are kept in in working order.

Stormshield Endpoint Security is easy to administer and quick to deploy, even when the PC installed base is very sizeable. It adapts to physical and virtual servers and has a light memory footprint. Several security layers are integrated, but a single agent is deployed for each server. Application controls, a firewall and network IDS prevent the destruction and leakage of data. The unique technology developed by Stormshield includes a continuous behavioral analysis of executables in order to detect anomalies.

Rootkits, key logging and attempts to elevate privileges are blocked. This is a proven method of protection against targeted attacks and APTs (Advanced Persistent Threats).



End of security patches = System at risk

ISSUES

Stormshield Endpoint Security = Proactive protection

SOLUTION

Level of security maintained = Server protected

RESULT

STORMSHIELD

Arkoon and Netasq, fully owned subsidiaries of Airbus Defence and Space, run the Stormshield brand and offer innovative end-to-end security solutions to protect networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security).

WWW.STORMSHIELD.EU